REMARKS

Claims 1, 2, and 4-16 are currently pending in the present application. Reconsideration and reexamination of the claims are respectfully requested.

The Examiner rejected Claims 1-16 under 35 U.S.C. 103 as being unpatentable over Jones (U.S. patent No. 5,412,730) in view of Lynn (U.S. patent no. 5,345,508) and further in view of Dent (U.S. patent no. 5,060,266). This rejection respectfully traversed with respect to the pending claims.

The features and advantages of the present invention were previously communicated to the Examiner:

The present invention is directed to a secured cryptographic communications system in which the communication nodes of the system include a pseudo-random key generator for generating pseudo-random keys that can be used to encrypt/decrypt communication data. Because the cryptographic keys can be generated locally at each communication node, the keys need not be transported between the communication nodes and hence the communication system is not susceptible to compromise via interception of keys. In accordance with a preferred embodiment of the present invention, a cryptographic key based on pseudo-randomly generated numbers are provided once every key change period, starting from a predetermined reference initialization value (referred to as the crypto midnight date and time value in the specification).

In order to ensure that the pseudo-random key generators are providing the same keys at the same time, the pseudo-random key generators are initiated at the same exact time and are preferably periodically synchronized with each other thereafter. However, in reality, it is impractical to initialize the different units of pseudo-random key generators at the exact same time, especially if the units are located in different parts of the world. Although it is possible for the manufacturer to initialize the units at the same time at the factory, subscribers of the system may not wish to have the generators activated at the factory for reasons of fearing comprising the generated keys during the transportation or shipping of the pseudo-random key generators. It is

more secure to initialize the pseudo-random key generators after they have been delivered to their intended users.

One of the important advantages offered by the present invention is the ability to initialize the pseudo-random key generators at different times while ensuring that the pseudo-random key generators will generate the same pseudo-random keys at the same time. To accomplish this objective, an initialization unit is included in the pseudo-random key generators, wherein the initialization units (such as the time/key initialize device 108 shown in Fig. 1), upon activating the pseudo-random key generator, will check a current data and time against the crypto midnight initialization date and time (CMDT) and determine a difference between the two time values. Using the difference in timing values the initialization unit determines how many predetermined key change periods have passed since the initialization date and time, and cause the pseudo-random number generator of the pseudo-random key generator to cycle through the generations of pseudo-random numbers from the CMDT through the current time value, effectively bringing the pseudo-random key generator up to date and ready to generate accurate pseudo-random keys going forward.

As also previously communicated, Jones is directed to a encryption data system that is dependent upon "block counting" technique for generating cryptographic keys. As the Examiner repeatedly acknowledged, Jones does not disclose generating cryptographic keys based on sequences of time or periods of time. More importantly, Jones does not deal with the initialization of pseudo-random key generators to ensure that the different units can generate consistent keys while being activated at different times.

Applicants respectfully submit that neither Dent nor Lynn makes up for the deficiencies of Jones. Specifically, as previously communicated and apparently acknowledged by the Examiner, Dent is directed to a system for synchronizing encryption devices and for the resynchronization of a sender and a receiver unit should the two devices fall out of synchronization. Dent does not teach or suggest an initialization procedure such that pseudo-

random key generators may be activated at different times and still generate symmetrical keys for a given time value.

Lynn discloses a system whereby pseudorandom cryptographic keys are generated by both a transmitter and a receiver. The stated purpose of Lynn is to conserve processing resources by saving generated cryptographic keys that correspond to a given initialization vector (see col. 2, lines 19-33). In particular, as discussed in column 2, lines 58 to column 3, line 5:

> "Both the transmitter and receiver share a common secret key that has been communicated through some separate channel. The transmitter combines the secret key (which serves as a constant base value) with an Initialization Vector (IV), using an XOR operation to produce a temporal key. This temporal key is then used as an input to a pseudorandom number (PN) generator to produce a unique PN sequence of binary digits, for each new temporal key entered. . . . The initialization vector together with its corresponding PN sequence is then stored in a cache and the PC sequence is iteratively reused, as determined by a counter, to encrypt one or more plaintext messages."

In other words, each time the transmitter sends a message, an initialization vector is first sent to the receiver, which will combine the received initialization vector with the common secret key via and XOR operation, the result of which is inputted into the PN generator for generating a sequence of binary numbers for decrypting the received message. The initialization vector, along with the corresponding generated PN sequence binary number, is at the same time stored in a memory for later use. In the event an initialization vector is re-used by the transmitter at a later time, the receiver will simply retrieve the previously generated sequence binary number rather than performing the XOR operation and inputting the XOR result into the PN generator again.

In summary, Lynn discloses utilizing a sequence generator at both ends of a communication channel wherein the sequence generators will generate an unique output for each unique input, wherein the input is a XOR product of a common secret key and an initialization vector that is transmitted from the transmitter to the receiver each time a message is to be sent. To conserve processing resources, the initialization vectors are reused, and the generated

sequence numbers are stored in a cache for later retrieval rather than re-generating the sequence number.

In contrast, the present invention does not require transmitting an initialization vector value to the receiver each time a message is to be sent. An important advantage of the present invention is that, once the pseudorandom cryptographic key generators are initialized, identical cryptographic keys are automatically generated at both the receiver and the transmitter without any need to provide any additional inputs or "initialization vectors." However, to compensate for different initialization times of different generators, upon initialization a generator first checks the current time against the crypto-midnight time (i.e., the preset initialization time), and brings the generator to synchronization with the transmitter generator. For instance, if the crypto-midnight value is 12:00 a.m., and the current time upon initialization is 3:00 a.m., and if the predetermined key change period is 10 minutes, then the initialized generator will "fast forward" the generation of sequence numbers by 18 key change periods to bring the generator to synchronization with the system.

The above aspect of the invention as claimed is not disclosed in any of the references cited. The Examiner points to column 2, lines 48-53 of Lynn as teaching this feature of the present invention. However, that section of Lynn simply states: "It is therefore desirable that a high speed cryptosystem exhibit the property of self-synchronization between transmitter and receiver such that no additional recovery procedures are required to decode messages." As the Examiner can surely appreciate, this is nothing more than stating a general goal; it does not teach nor suggest the details of the present invention as claimed whatsoever. There is simply no teachings, by any of the references, of the initialization step as recited in all of the claims. Applicants therefore respectfully submit that none of the claims are obvious in view of the combination of the references cited.

In view of the foregoing, Applicants respectfully submit that all of the pending claims are in condition for allowance. Reconsideration and reexamination of the claims, as amended, are

respectfully requested. The Examiner is encouraged to telephone the undersigned attorney if doing so would advance the prosecution of the present application.

In the unlikely event that the transmittal letter is separated from this document and the Patent Office determines that an extension and/or other relief is required, Applicant petitions for any required relief including extensions of time and authorizes the Assistant Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to **Deposit Account No. 03-1952** referencing docket no. 578062000300.

Respectfully submitted,

Dated: May 4, 2005

By: _____

David T. Yang
Registration No. 44,415

Morrison & Foerster LLP
555 West Fifth Street
Suite 3500
Los Angeles, California 90013-1024
Telephone: (213) 892-5587
Facsimile: (213) 892-5454